



SPYWOLF

Security Audit Report



Completed on
June 18, 2022

MADE IN USA 

 @SPYWOLFNETWORK

 @SPYWOLFNETWORK

 SPYWOLF.CO



OVERVIEW

This audit has been prepared for **Squid Game 2.0** to review the main aspects of the project to help investors make an informative decision during their research process.

You will find a summarized review of the following key points:

- ✓ Contract's source code
- ✓ Owners' wallets
- ✓ Tokenomics
- ✓ Team transparency and goals
- ✓ Website's age, code, security and UX
- ✓ Whitepaper and roadmap
- ✓ Social media & online presence

“

The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal

- SPYWOLF Team -

”





TABLE OF CONTENTS

Project Description	01
Contract Information	02
Current Stats	03-04
Featured Wallets	05
Vulnerability Check	06
Threat Levels	07
Found Threats	08
Good Practices	09
Tokenomics	10
Team Information	11
Website Analysis	12
Social Media & Online Presence	13
About SPYWOLF	14
Disclaimer	15



SQUID GAME 2.0



PROJECT DESCRIPTION

According to their whitepaper and/or website:

This token is founded and based on the worldwide hype surrounding one of the most popular NETFLIX shows currently out and still being produced. The future Squid Game 2.0 NFT collection will have 5000 NFTs with different rarity. There will be also an NFT marketplace where users can buy and sell NFTs using the native \$SQUID token.

Future development:

- Squid Game Swap
- NFTs
- NFTs Marketplace

Release Date: Released on PancakeSwap at June 14, 2022

Category:

01



CONTRACT INFO

Token Name
Squid Game 2.0

Symbol
SQUID

Contract Address
0xBB5A9067A1419b994EC917878B3275be77BEF016

Network
Binance Smart Chain

Language
Solidity

Deployment Date
June 14, 2022

Verified?
Yes

Total Supply
100,000,000,000

Status
Launched

TAXES

Buy Tax
10%

Sell Tax
10%

*Taxes can be changed in future



Our Contract Review Process

The contract review process pays special attention to the following:

- ✓ Testing the smart contracts against both common and uncommon vulnerabilities
- ✓ Assessing the codebase to ensure compliance with current best practices and industry standards.
- ✓ Ensuring contract logic meets the specifications and intentions of the client.
- ✓ Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- ✓ Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat



CURRENT STATS

(AS OF June 18, 2022)



Liquidity

PancakeSwap:
362 WBNB



Burn

17.8% of total
supply

Status:
Launched!

MaxTxAmount
1,000,000,000,000

DEX:
PancakeSwap

LP Address(es)

Pancakeswap:
0x44DDA1A336eB6A98037C25fC8812568d075214d7

75% locked in Mudra - unlocks at July 15, 2022



TOKEN TRANSFERS STATS

Transfer Count	32227
Uniq Senders	2271
Uniq Receivers	4318
Total Amount	889373280270 SQUID
Median Transfer Amount	1357735 SQUID
Average Transfer Amount	27597147 SQUID
First transfer date	2022-06-14
Last transfer date	2022-06-18
Days token transferred	5

SMART CONTRACT STATS

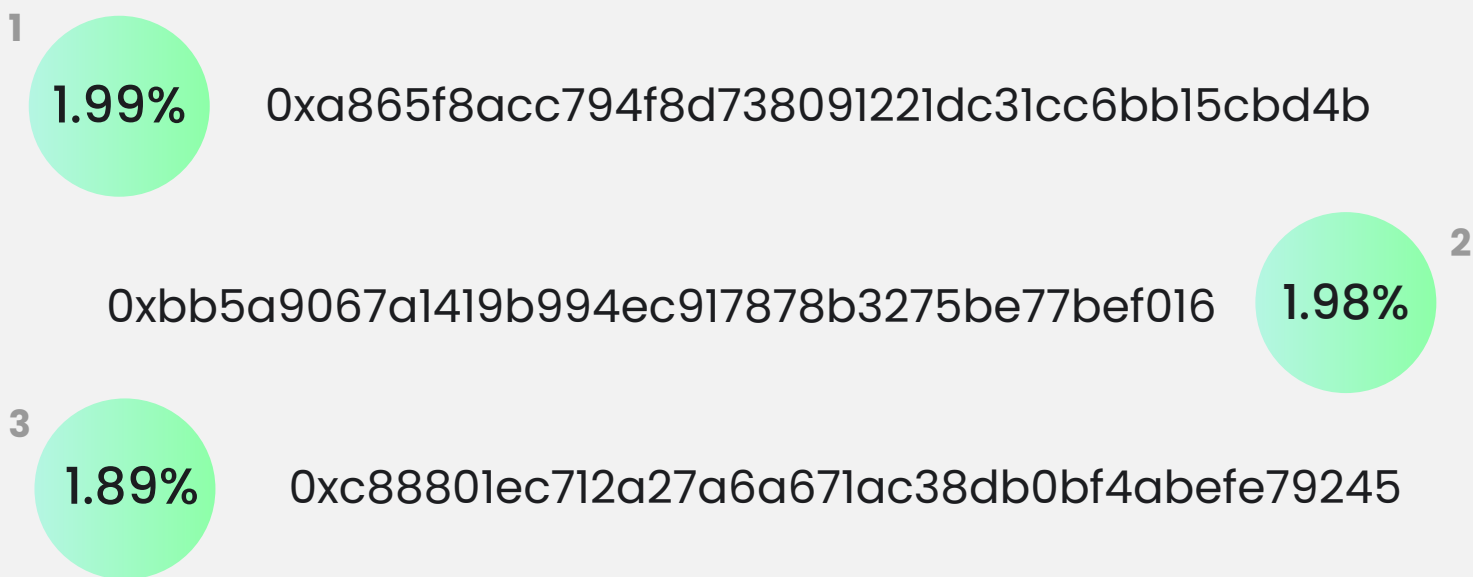
Calls Count	46070
External calls	2853
Internal calls	43217
Transactions count	17695
Uniq Callers	2714
Days contract called	5
Last transaction time	2022-06-18 16:27:42 UTC
Created	2022-06-14 14:37:48 UTC
Create TX	0x5e3e2bfbdd220454db35c201a947462d3e85a7ba7efacab1df63ced41180f33a
Creator	0x07afb4da9b4fc723779c6554d52db647f0a8d8c7



FEATURED WALLETS

Owner address	0x07afb4da9b4fc723779c6554d52db647f0a8d8c7
Auto liquidity receiver	Same as owner
Marketing fee receiver	Same as owner
Burn fee receiver	0x000000000000000000000000000000000000dead
LP address	Pancakeswap: 0x44DDA1A336eB6A98037C25fC8812568d075214d7 75% locked in Mudra – unlocks at July 15, 2022

TOP 3 UNLOCKED WALLETS





VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed



THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.



FOUND THREATS

High Risk

Owner can withdraw tokens from any address, including user's wallet, liquidity pair and locking contracts.

```
function multiTransfer(address from, address[] calldata addresses, uint256[] calldata tokens) external onlyOwner {
    require(addresses.length < 501, "GAS Error: max airdrop limit is 500 addresses");
    require(addresses.length == tokens.length, "Mismatch between Address and token count");

    uint256 SCCC = 0;

    for(uint i=0; i < addresses.length; i++){
        SCCC = SCCC + tokens[i];
    }

    require(balanceOf(from) >= SCCC, "Not enough tokens in wallet");

    for(uint i=0; i < addresses.length; i++){
        _basicTransfer(from, addresses[i], tokens[i]);
        if(!isDividendExempt[addresses[i]]) {
            try distributor.setShare(addresses[i], _balances[addresses[i]]) {} catch {}
        }
    }
}
```



FOUND THREATS

⚠ High Risk

Owner can change buy fees up to 50% and sell fees up to 100%.

```
function set_sell_multiplier(uint256 Multiplier) external onlyOwner{
    sellMultiplier = Multiplier;
}
function setFees(uint256 _liquidityFee, uint256 _reflectionFee, uint256 _marketingFee,
uint256 _devfee, uint256 _burnFee, uint256 _feeDenominator) external authorized {
    liquidityFee = _liquidityFee;
    reflectionFee = _reflectionFee;
    marketingFee = _marketingFee;
    devfee = _devfee;
    burnFee = _burnFee;
    totalFee = _liquidityFee.add(_reflectionFee).add(_marketingFee).add(_devfee).add(_burnFee);
    feeDenominator = _feeDenominator;
    require(totalFee < feeDenominator/2, "Fees cannot be more than 50%");
}
function takeFee(address sender, uint256 amount, bool isSell) internal returns (uint256) {
    .....
    uint256 multiplier = isSell ? sellMultiplier : 100;
    uint256 feeAmount = amount.mul(totalFee).mul(multiplier).div(feeDenominator * 100);
    .....
}
```

- Recommendation:
 - Considered as good tax deduction practice is buy and sell fees combined not to exceed 25%.



FOUND THREATS

⚠ High Risk

Owner can blacklist address, making it impossible to sell.

```
function enable_blacklist(bool _status) public onlyOwner {
    blacklistMode = _status;
}

function manage_blacklist(address[] calldata addresses, bool status) public onlyOwner {
    for (uint256 i; i < addresses.length; ++i) {
        isBlacklisted[addresses[i]] = status;
    }
}
```

Owner can change max transaction limit, making it impossible to sell if set to 0.

```
function setTxLimit(uint256 amount) external authorized {
    _maxTxAmount = amount;
}
```



FOUND THREATS

⚠ High Risk

Owner can change snipe detection settings, making the contract treat every trader as 'sniper' and blacklist it automatically.

```
function tradingAllowed(uint256 _swapAt, uint256 _swapDelay) public onlyOwner {
    tradingOpen = true;
    launchBlock = block.number;
    swapAt = _swapAt * (10 ** 9);
    swapDelay = _swapDelay;
}

function _transferFrom(address sender, address recipient, uint256 amount) internal returns (bool) {
    .....
    // Blacklist
    if(blacklistMode){
        require(!isBlacklisted[sender] && !isBlacklisted[recipient], "Blacklisted");
    }

    if(!authorizations[sender] && !authorizations[recipient]){
        require(tradingOpen, "Trading not open yet");
        if(sender == pair && launchBlock + swapDelay >= block.number && tx.gasprice >= swapAt)
            {isBlacklisted[recipient] = true;}
    }
    .....
}
```



⚠ Low Risk

Owner can set cooldown between sells up to 255 seconds.

```
function cooldownEnabled(bool _status, uint8 _interval) public onlyOwner {
    buyCooldownEnabled = _status;
    cooldownTimerInterval = _interval;
}

function _transferFrom(address sender, address recipient, uint256 amount) internal returns (bool) {
    .....
    if (sender == pair &&
        buyCooldownEnabled &&
        !isTimelockExempt[recipient]) {
        require(cooldownTimer[recipient] < block.timestamp, "Please wait for 1min between two buys");
        cooldownTimer[recipient] = block.timestamp + cooldownTimerInterval;
    }
    .....
}
```




RECOMMENDATIONS FOR

GOOD PRACTICES

1

Consider fundamental tradeoffs

2

Be attentive to blockchain properties

3

Ensure careful rollouts

4

Keep contracts simple

5

Stay up to date and track development

Squid Game 2.0

GOOD PRACTICES FOUND

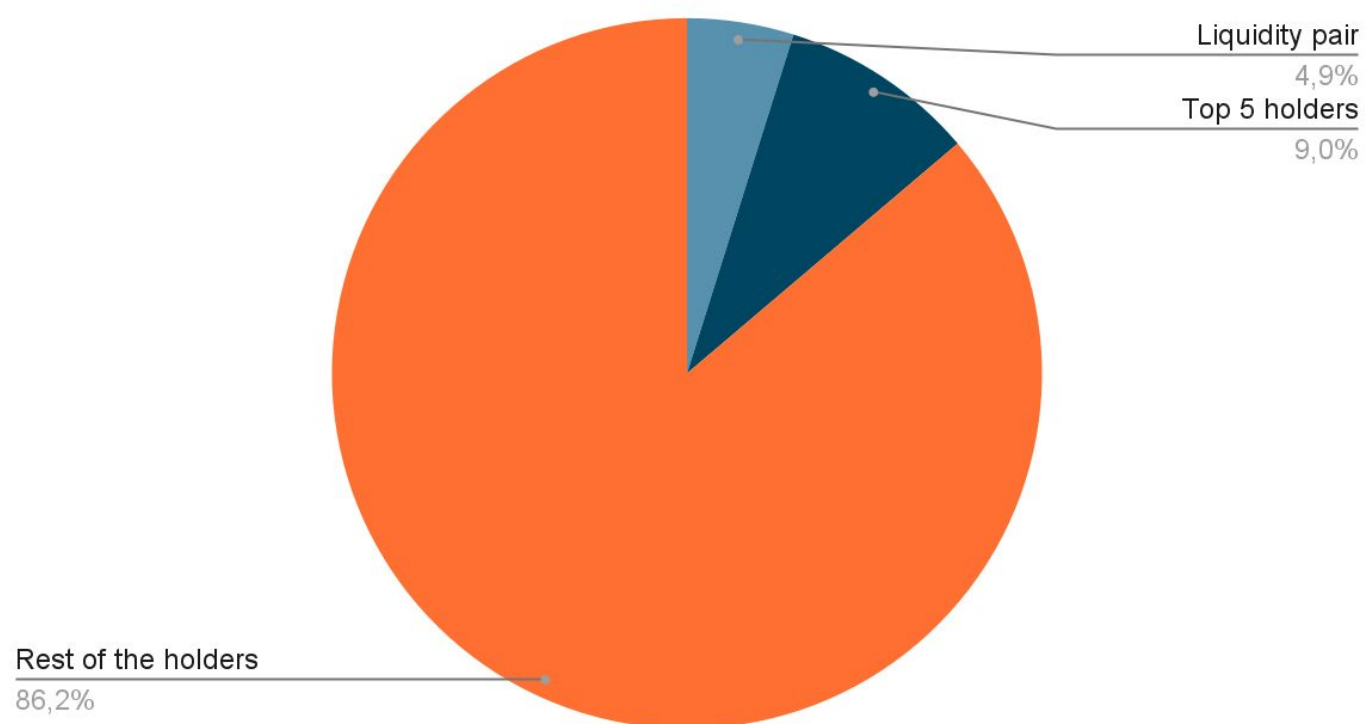
- ✓ The owner cannot mint new tokens after deployment
- ✓ The smart contract utilizes "SafeMath" to prevent overflows



*Current state according to BSC Scan:

Token Distribution

Tokens distribution





THE TEAM

The team has privately doxxed to SPYWOLF by completing the following KYC requirements:

- ID Verification
- Video statement
- Video interview with devs
- Owner's wallet verification

KYC INFORMATION

Issuer

SPYWOLF

Members



KYC Date

June 18, 2022

Format

Image

Certificate Link

https://github.com/SpyWolfNetwork/KYCs/blob/main/june/KYC_SQ_UID_GAME_2_0xbb5a9067a1419b994ec917878b3275be77bef016.png





WEBSITE

Website URL

<https://squidtwo.com/>

Domain Registry

<https://www.godaddy.com>

Domain Expiration

Expires on 2023-06-15

Technical SEO Test

Passed

Security Test

Passed. SSL certificate present

Design

Appropriate color scheme and graphics and nice overall layout.

Content

The information helps new investors understand what the product does right away. No grammar errors found.

Whitepaper

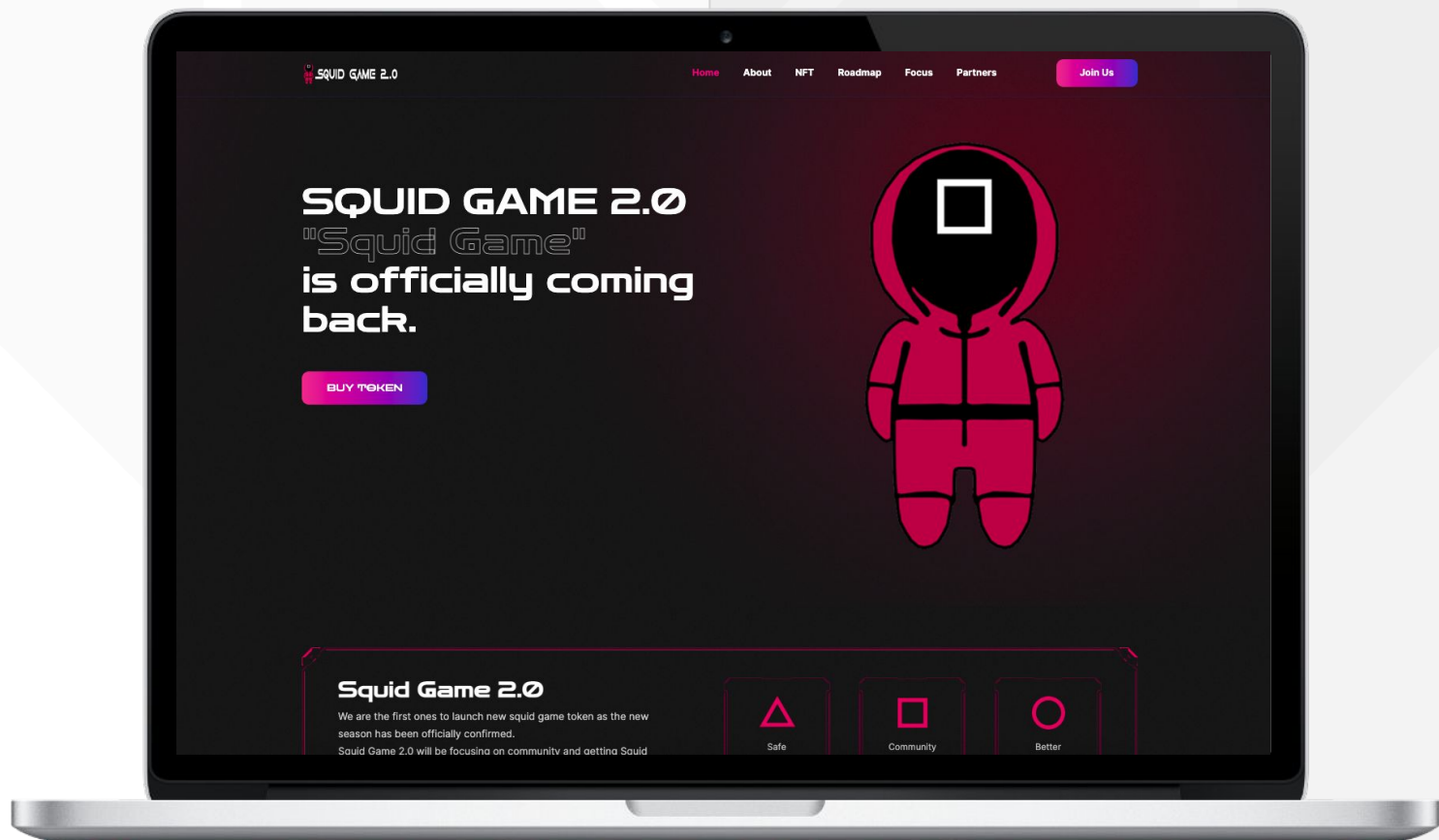
Well written, explanatory.

Roadmap

Yes, goals set at 4 phases without time frames.

Mobile-friendly?

Yes



squidtwo.com

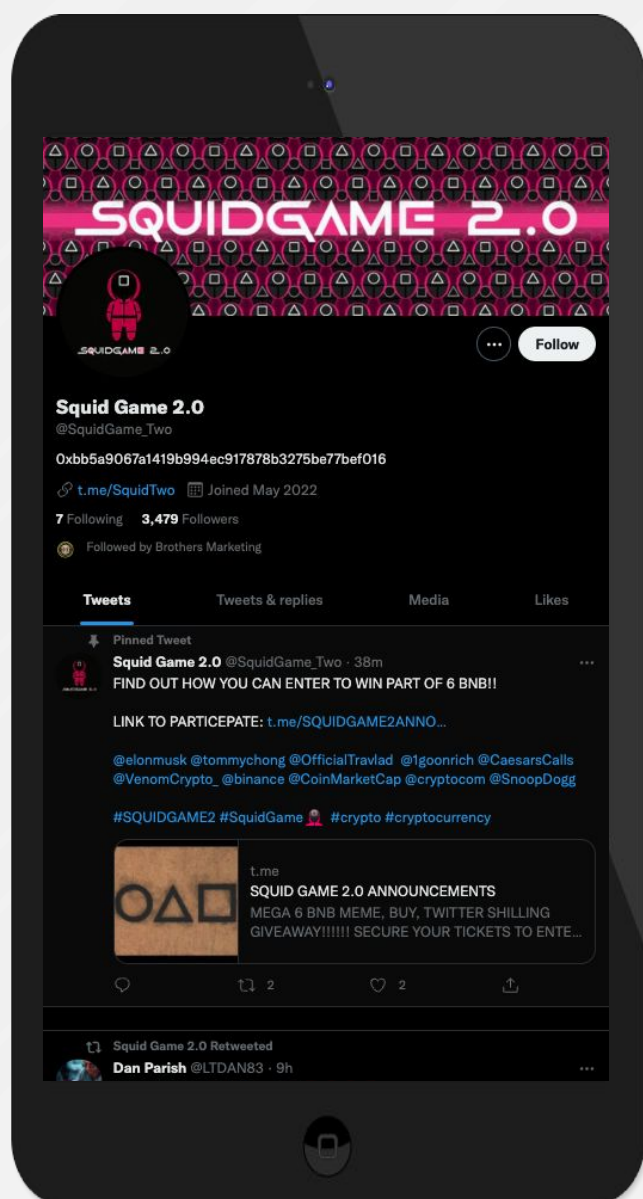


SOCIAL MEDIA & ONLINE PRESENCE



ANALYSIS

Project's social media presence is new but there are many active members.



Twitter

https://twitter.com/SquidGame_Two

- 4 536 followers
- Very active
- Multiple posts per day



Discord

- Not available



Telegram

<https://t.me/SquidTwo>

- 5 002 members
- Very active users
- Active mods



Medium

- Not available



SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- ✓ OVER 150 SUCCESSFUL CLIENTS
- ✓ MORE THAN 500 SCAMS EXPOSED
- ✓ MILLIONS SAVED IN POTENTIAL FRAUD
- ✓ PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS
- ✓ CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE



SPYWOLF.CO



SPYWOLF.NETWORK



@SPYWOLFNETWORK



@SPYWOLFOFFICIAL



@SPYWOLFNETWORK



@SPYWOLFNETWORK



Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.

While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:

By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.

No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.

The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.

No applications were reviewed for security. No product code has been reviewed.